International Journal of Computer Science Engineering
and Information Technology Research (IJCSEITR)
ISSN(P): 2249-6831; ISSN(E): 2249-7943
Vol. 3, Issue 5, Dec 2013, 165-170
© TJPRC Pvt. Ltd.

A NOVEL TECHNIQUE FOR DWT-SVD BASED SECURED IMAGE WATERMARKING

MANOJ KUMAR RAMAIYA[1], NIRUPMA TIWARI[2], NAVEEN HEMRAJANI[3] & RICHA MISHRA[4]

[1,2]Research Scholar, Department of Computer Science, Suresh Gyanvihar University, Jaipur, Rajasthan, India

[3]Professor, Department of Computer Science, Suresh Gyanvihar University, Jaipur, Rajasthan, India

[4]Department of Computer Science & Engineering, Shriram College of Engg & Mgmt, Gwalior, Madhya Pradesh, India

ABSTRACT

Proposed paper present a new robust watermarking technique for copyright protection based on Discrete Wavelet Transform and Singular Value Decomposition. The Low frequency sub band of the wavelet decomposed cover image is modified by modifying its singular values. A secret key is generated from the original watermark with the help of visual cryptography to claim the ownership of the image. The ownership of the image can be claimed by superimposing this secret key on the extracted watermark from the watermarked image. The robustness of the technique is tested by applying different attacks and the visual quality of the extracted watermark after applying these attacks is good. Also, the visual quality of the watermarked image is indistinguishable from the original image.

KEYWORDS: Image Watermarking, Visual Cryptography, Singular Value Decomposition, Discrete WaveletTransform, Robustness, Steganography

INTRODUCTION

Introduction Digital information is easy to distribute, duplicate and modify which leads to the need for copyright protection techniques. Digital watermarking technique is one of the solutions to avoid unauthorized copying or tampering of multimedia data. Recently many watermarking schemes have been proposed to address this problem. The watermarking schemes are broadly categories into two main domains i.e. spatial domain and the transform domain. In spatial domain watermarking the watermark is embedded by directly modifying the intensity values of the cover image. The most popular technique is the least significant bit (LSB) method. In transform domain the watermark is embedded by modifying the frequency coefficients of the transformed image. The common methods in the transform domain are Fourier transform (DFT), discrete cosine transform (DCT), discrete wavelet transform (DWT), etc. Recently, singular value decomposition (SVD) was explored for watermarking. It is one of the most useful numerical analysis techniques having property that the singular values (SVs) of an image do not change significantly when a small perturbation is added to an image. [1-4]. With the rapid development of internet technology, transmission of multimedia information over the Internet becomes convenient. While transmitting these data security of multimedia data is a prime concern.

RELATED WORKS

The hackers may steal information to misuse this important data. Hence secret images are generated before this transmission. One of the solutions to deal with this security problems is Visual cryptography. Naor and Shamir had introduced Visual cryptography

Chin-Chen Chang et al [6]suggested spatial-domain image hiding schemes to hide a binary watermark into two shares. The two different gray level cover images are used to embed these secret shares. Embedding images can be superimposed to decode the hidden messages. To balance the performance between pixel expansion and contrast, Liguo

Fang [7] proposed scheme based on combination. Xiao-qing and Tan [8] has suggested a threshold visual secret sharing schemes based on binary linear error correcting code. The author has mixed XOR and OR operation with reversing. VC-based repeating watermarking scheme is proposed by Wang, Tai, and Yu [9]. The authors add some parts of the watermark into edge blocks of the host image. It results in enhance robustness of the scheme. The limitation of the scheme is that the host image must be altered to embed a watermark.

In presentpaper, we apply the concept of Singular Value Decomposition to embed a watermark into the cover image and to extract this watermark from the watermarkedimage. The watermark to be embedded is encrypted using visual cryptography. The watermark is first split into two shares. However, only the first share acts as a watermark while the second share acts as the secret key. Thus, the other share is the key to reconstruct the watermark.. The scheme is robust after several attacks are performed on the watermarked image. Section 2 gives preliminaries used for the proposed technique. Section 3 presents the technique for splitting a watermark using visual cryptography and embedding and extraction of the share. The experimental results and discussion is given in Section 4 followed by conclusion in Section 5.

PROPOSED ALGORITHM

The proposed technique is divided in two sections, embedding technique and the extraction technique as follow.

Embedding Technique

Step1: Apply 1-level DWT on the cover image. It gives four subbands LL, LH, HL, and HH. The LL sub band is selected for the embedding of watermark as the high frequency coefficient changes are responsible for the changes in the edges only.

Step2: SVD is calculated for LL sub band only. This will reduce the computational overhead as we are not considering the whole cover image.

CD1=CU+CS+CV’

Step3: The watermark is now encrypted to increase the security of the scheme. For this we applied the visual cryptography on the watermark. This will divide the watermark into two shares, viz., share 1 and share 2. The original watermark can be obtained if both the shares of the encrypted watermark are superimposed on each other. Hence we will use share1 of the watermark for the embedding purpose while share 2 of the watermark is provided as the secret key.

Step4: Apply SVD on the share1 of the watermark

Wshare1=WU+WS+WV’

Step5: Modify the singular values of the HH subband of cover image and apply inverse SVD.

W1=CS+αWS

Where, CS is the SV’s of the cover image and WS are the SV’s of the watermark.α is the embedding strength. CD1’=CU+W1+CV’

Step6: Perform the inverse DWT by combining the subbands with the modified one to get the watermarked image.

The embedding technique is shown in following figure 1

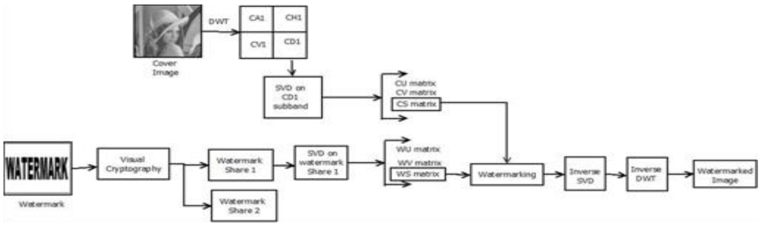

Figure 1: Embedding Technique

Extraction Technique

The extraction technique is exactly the reverse of the embedding technique.

- Perform level-1 DWT on watermarked image.
- Perform SVD on the LL sub band.
- Extract the singular values of the watermark.

  WSextract= (W1-CS)/α
- Perform inverse SVD to get the share 1 of the decrypted watermark1 i.e. share 1 of the watermark.
- Share 2 which acts as secret key is superimposed on the decrypted watermark share 1 to get the extracted watermark.

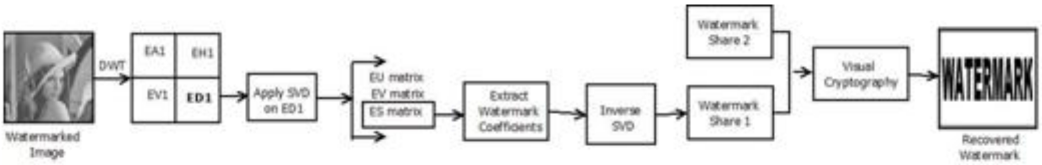

Figure 2: Extraction Technique

SIMULATION RESULT

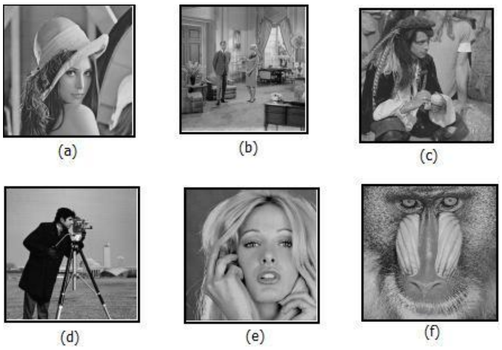

Figure 3: Cover Images (A) Lena (B) Living Room (C) Pirate (D) Cameraman (E) Woman (F) Mandrill

In order to authenticate the performance of the proposed technique, simulation is done on wide set of cover images and watermarks using MATLAB10. The cover image is of size 512X512 gray scale images as shown in figure 3 and watermark is of size 256 X 256 as shown in figure 4. As indicated in figure 4 the watermark is divided into two shares after applying visual cryptography. This is represented as visual crypt watermark 1 and 2 respectively. The decrypted watermark 1 is the share 1 of the watermark extracted from the watermarked images. This is combined with the visual crypt watermark 2 to get the extracted watermark.

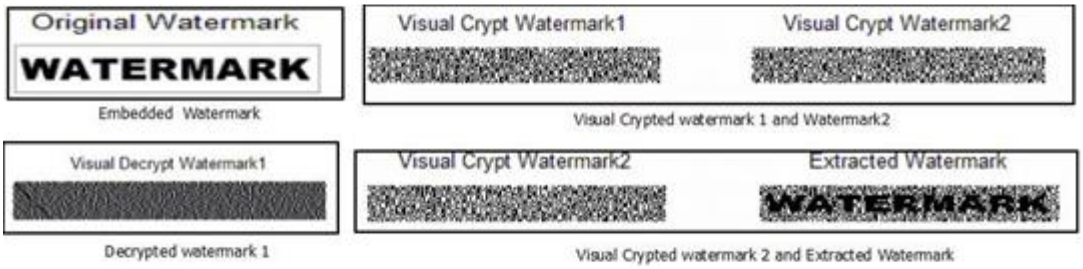

Figure 4: Embedded and Extracted Watermark

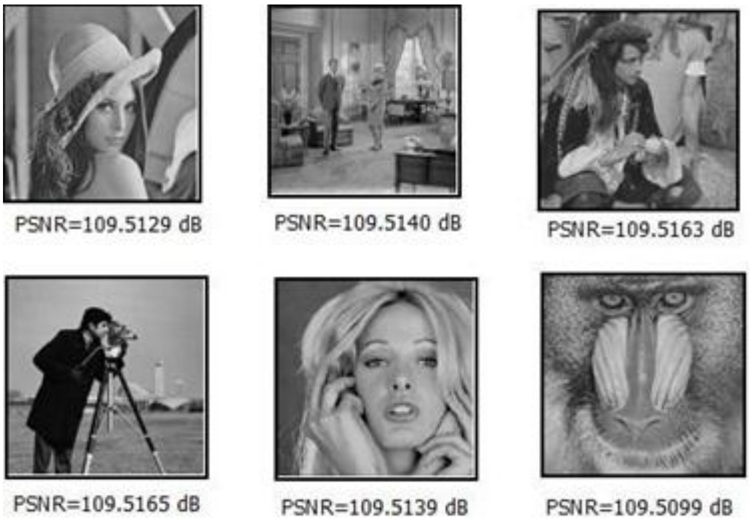

Figure 5: Watermarked Images with PSNR

Above Figure-5 shows the PSNR obtained between cover image and watermarked image for all standard test images. The PSNR indicates that the imperceptibility of the watermarked image is good and the watermarked image is indistinguishable from the cover image. To check the robustness of our algorithm we applied a wide set of attacks on the test images. The effect of these attacks on the watermark images with corresponding extracted decrypted watermark and extracted watermark by combining the share 2 of the watermark.

The visual quality of the extracted watermark is good after applying the different attacks. This acceptable performance is measured with the help of normalized correlation measured between embedded and extracted watermark. Table 1 shows the normalized PSNR values after applying different attacks on the watermarked images.

Table 1: Normalized Correlation Between Embedded and Extracted Watermark

Image Attacks	Lena	Goldhill	Pepper	Cameraman	Baboon
Cropping	36.98	36.98	36.97	36.98	36.98
Image Intensity	36.98	36.98	36.98	36.98	36.99
Speckle Noise	36.99	36.98	36.98	36.99	36.98
Gaussian Noise	36.98	36.98	36.98	36.98	36.98
Rotation	36.98	36.98	36.98	36.98	36.98
Histogram Equalization	36.98	36.98	36.98	36.98	36.98
Salt & Pepper Noise	36.98	36.98	36.98	36.98	36.98
Gaussian filter	36.98	36.98	36.98	36.98	36.98
Resize	36.98	36.98	36.98	36.98	36.98
JPEG	36.98	36.98	36.98	36.98	36.98
Motion Blurred	36.98	36.98	36.98	36.98	36.98

CONCLUSIONS

In this paper a new robust watermarking technique for copyright protection has been proposed. We applied the singular value decomposition along with the Discrete Wavelet Transform. Since the technique utilizes the properties of both DWT and SVD the proposed technique is more robust against different attacks. The innovation of this paper is that the security of the algorithm is increased with the help of visual cryptography on the watermark image. If the second share of the watermark which acts as the key is not present then it is not possible to extract the exact watermark information. It is very difficult to change or remove the watermark without knowing the secret key share as the watermark is split into two shares with random patterns. The robustness of the technique is justified by giving analysis of the effect of attacks and still we are able to get good visual quality of the embedded watermark.

ACKNOWLEDGEMENTS

The authors' acknowledgment is due to Dr. Anil Kishore Saxena , Director, ShriRam College of Engg. & Mgmt. (SRCEM) for the all time encouragement and blessing to carry the research.

REFERENCES

1. R. Sun, H. Sun, and T. Yao, "A SVD and quantization based semifragile watermarking technique for image authentication," in Proc.Int. Conf. Signal Process., pp. 1592–1595, (2002)

2. C. C. Chang, P. Y. Tsai, and M. H. Lin, "SVD-based digital image watermarking scheme," Pattern Recogn. Lett. 26, 1577–1586, (2005).

3. J. M. Shieh, D. C. Lou, and M. C. Chang, "A semi-blind digital watermarking scheme based on singular value decomposition," Comput. Stand. Inter. 28, 428–440, (2006).

4. R. Liu and T. Tan, "An SVD-based watermarking scheme for protecting rightful ownership," IEEE Trans. Multimedia 4, 121–128, (2002).

5. Moni Naor and Adi Shamir, "Visual Cryptography", advances in cryptology– Eurocrypt, pp 1-12, (1995).

6. Chin-Chen Chang, Jun-Chou Chuang, Pei-Yu Lin , "Sharing A Secret Two-Tone Image In Two Gray-Level Images", Proceedings of the 11th International Conference on Parallel and Distributed Systems , ICPADS'05, (2005).

7. Liguo Fang, BinYu, "Research On Pixel Expansion Of (2,n) Visual Threshold Scheme", 1st International Symposium on Pervasive Computing and Applications, pp 856-860, (2006)

8. Xiao-qing Tan, "Two Kinds Of Ideal Contrast Visual Cryptography Schemes", International Conference on Signal Processing Systems, pp. 450-453,(2009)

9. C. C. Wang, S. C. Tai, and C. S. Yu, "Repeating image watermarking technique by the visual cryptography," IEICE Trans. Fundamentals E83-A_8_, 1589–1598, (2000).

10. C. C. Chang and J. C. Chuang, "An image intellectual property protection scheme for gray-level images using visual secret sharing strategy," Pattern Recogn. Lett. 23, 931–941, (2002).

11. D. C. Lou, J. M. Shieh, and H. K. Tso, "Copyright protection scheme based on chaos and secret sharing techniques," Opt. Eng. 44_11_, 117004, (2005).

12. C. S. Hsu and Y. C. Hou, “Copyright protection scheme for digital images using visual cryptography and sampling methods,” Opt. Eng.44_7_, 077003, (2005).